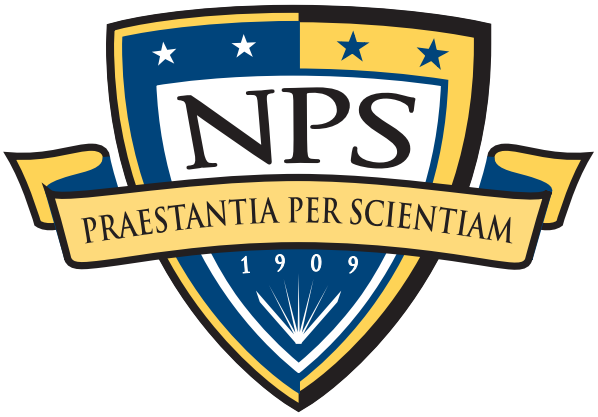

NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

SECRET SHARING SCHEMES AND ADVANCED ENCRYPTION STANDARD

by

Bing Yong Lim

September 2015

Thesis Advisor:	Pantelimon Stanica
Second Reader:	David Canright

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE

Form Approved OMB No. 0704–0188

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202–4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.

1. AGENCY USE ONLY *(Leave Blank)*	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	September 2015	Master's Thesis 09-29-2014 to 09-25-2015

4. TITLE AND SUBTITLE

SECRET SHARING SCHEMES AND ADVANCED ENCRYPTION STANDARD

5. FUNDING NUMBERS

6. AUTHOR(S)

Lim, Bin Yong

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Naval Postgraduate School
Monterey, CA 93943

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)

N/A

10. SPONSORING / MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES

The views expressed in this document are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government. IRB Protocol Number: N/A.

12a. DISTRIBUTION / AVAILABILITY STATEMENT

Approved for public release; distribution is unlimited

12b. DISTRIBUTION CODE

13. ABSTRACT *(maximum 200 words)*

The major objective of this study is to identify a simplified methodology to reconstruct a secret that is distributed using Shamir's Secret Sharing Scheme, and to use the derived results to investigate implications on Advanced Encryption Standard. This thesis begins by using existing mathematical conjectures to simplify a monic polynomial generated by the dealer in a threshold secret sharing scheme. The second part of the thesis then identifies the variable bounds that an individual (eavesdropper or outsider) can use to reconstruct the secret by gathering just two shares out of multiple public shares. In conclusion, the findings from the first two parts of the simplified secret sharing scheme can be effectively used to identify weaknesses of side-channel attacks, and subsequently applied to improve on the mechanics of Advanced Encryption Standard. Future work could include generalizing the methodology to include non-monic polynomials, or exploring the use of prime coefficients in the dealer-generated polynomial.

14. SUBJECT TERMS

secret sharing, secret reconstruction, monic polynomials, Advanced Encryption Standard

15. NUMBER OF PAGES 61

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
Unclassified	Unclassified	Unclassified	UU

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2–89)
Prescribed by ANSI Std. 239–18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

SECRET SHARING SCHEMES AND ADVANCED ENCRYPTION STANDARD

Bing Yong Lim
Major, Republic of Singapore Air Force
B.S., Nanyang Technological University, 2004

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN APPLIED MATHEMATICS

from the

NAVAL POSTGRADUATE SCHOOL
September 2015

Author: Lim Bing Yong

Approved by: Dr. Pantelimon Stanica
Thesis Advisor

Dr. David Canright
Second Reader

Dr. Craig Rasmussen
Chair, Department of Applied Mathematics

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

The major objective of this study is to identify a simplified methodology to reconstruct a secret that is distributed using Shamir's Secret Sharing Scheme, and to use the derived results to investigate implications on Advanced Encryption Standard. This thesis begins by using existing mathematical conjectures to simplify a monic polynomial generated by the dealer in a threshold secret sharing scheme. The second part of the thesis then identifies the variable bounds that an individual (eavesdropper or outsider) can use to reconstruct the secret by gathering just two shares out of multiple public shares. In conclusion, the findings from the first two parts of the simplified secret sharing scheme can be effectively used to identify weaknesses of side-channel attacks, and subsequently applied to improve on the mechanics of Advanced Encryption Standard. Future work could include generalizing the methodology to include non-monic polynomials, or exploring the use of prime coefficients in the dealer-generated polynomial.

THIS PAGE INTENTIONALLY LEFT BLANK

Table of Contents

List of Tables

THIS PAGE INTENTIONALLY LEFT BLANK

List of Acronyms and Abbreviations

AES	Advanced Encryption Standard
DFT	Discrete Fourier Transformation
D-H	Diffie-Hellman
DoD	Department of Defense
FIPS PUBS	Federal Information Processing Standards Publications
NPS	Naval Postgraduate School
RSA	Rivest-Shamir-Adleman
SCA	side-channel analysis
SNR	signal-to-noise ratio
SSSS	Shamir's Secret Sharing Scheme
WLOG	Without loss of generality
XOR	exclusive-or

THIS PAGE INTENTIONALLY LEFT BLANK

Executive Summary

There are many secret sharing schemes and variations available to hide and reconstruct the given secret. Shamir's Secret Sharing Scheme, making use of linear Lagrange interpolation on the dealer-generated polynomial, was used to reconstruct the secret from the stipulated threshold number of participants' shares. Such a scheme had been widely analysed by mathematicians and computer scientists for potential weaknesses in the reconstruction of the secret by an external eavesdropper.

The objective of this thesis report is thus to present a variation of Shamir's threshold secret sharing scheme by manipulating the dealer-generated polynomial into a simplified version such that any eavesdropper can reconstruct the secret by gaining two public shares, instead of the stipulated threshold level. The envisaged improvements would then be evaluated for any impact on side-channel effects on the Advanced Encryption Standards.

Existing and famous mathematical conjectures (including Pillai's conjecture, the Fermat-Catalan conjecture, and Hall's conjecture) were built upon to seek a potential weakness in the security of the current secret sharing scheme. Essentially, the analysis aimed to reduce the order of difficulty in reconstructing the secret. Assuming that the dealer-generated polynomial is monic, it is then deconstructed by applying a composite linear function in which two additional variables are introduced.

In general, assuming that the original form of the dealer-generated polynomial is $f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_{k-1}x^{k-1}$, by composing it with the linear function $g(x) = x + \alpha$, the eventual form of the dealer-generated polynomial can be manipulated to be in the form of $f(x) = (x+\alpha)^k - b_0$, where both α and b_0 are the two newly introduced variables. The challenge then is reduced to finding the values of both α and b_0.

It was postulated that an eavesdropper would be able to recover the secret by simply obtaining two public shares, namely (x_1, y_1) and (x_2, y_2), from the multitude of available public shares, and this could be achieved by determining the numerical boundaries for the variable α. Specifically, all encompassing cases, without loss of generality, were considered to ensure that all possibilities were not neglected. The start state would be to take the difference between the two y-values that were easily obtained. From there on, it is just a matter of

manipulating the inequalities to screen out the boundaries of α. Once the boundaries of α were found, then it would be trivial to try out the available choices for α, and subsequently b_0, and eventually the secret.

While this methodology does not allow for the absolute reconstruction of the secret as compared to Lagrange interpolation, it presents an alternate methodology for an eavesdropper to retrieve the secret using shares that are significantly less than the required threshold number. The boundaries reduced the possibilities of the secret value from a near-infinite number to a manageable cardinality size that could be derived through exhaustive means. The crux is that as long as two shares are gathered together, the value of α can be derived easily through exhaustive means. Once the value of α is found, then it remains trivial to determine b_0 through the equation $y_i = (x_i + \alpha)^k - b_0$, where (x_i, y_i) are known public shares. Subsequently, the secret is reconstructed to be $f(0)$.

Therefore, it is important for the dealer to generate the polynomial with coefficients that do not contain a common factor. From this thesis analysis, it was concluded that the common factor, if accidentally found by an eavesdropper or outsider, can be used to reconstruct the secret efficiently by using only two public shares.

Such findings pave the way for an alternate methodology to recover the secret with less-than-expected available information. It effectively reduces the order of evaluating the monic polynomial, since only linear algebra is involved. This stems from the motivation that linear equations are easier to solve, and in cryptography, linearity presents a less security form for any eavesdropper to break through. Thus, for improved security, the dealer should avold generating the polynomial using successive binomial integers as its polynomial coefficients, further amplifying the importance of the dealer.

A lot of research had been focused on the *perfect* secret sharing scheme. While there are no known weaknesses to Shamir's Secret Sharing Scheme, many researchers had focused on the computational inefficiency if the generated polynomial comprises large degrees. While many improvised secret sharing schemes have proven more effective than Shamir's Secret Sharing Scheme, they have only been better under certain parameters; there is always a trade-off with some parameter of the scheme.

Acknowledgments

Without a doubt, I am heavily indebted to Dr. Pante Stanica, professor and associate chair of research in the Department of Applied Mathematics, Naval Postgraduate School, who graciously agreed to be my thesis advisor when I first approached him. Throughout the period of my thesis research, Dr. Stanica has shown the utmost patience and provided invaluable guidance to me. I shall never forget the advice that Dr. Stanica first gave to me, urging me that while generating a credible thesis is of utmost priority for the completion of the master's course, it is equally important to continue to learn something new along my academic journey.

I would also like to thank Dr. David Canright for pointing me in the right direction on related cryptography topics. His expertise in Advanced Encryption Standard allowed me to reach a deeper level of understanding for the second part of my thesis. Special mention goes to Associate Professor Ralucca Gera, who imparted me with the domain knowledge in discrete mathematics, and graph/network theory. Most importantly, she introduced me to the LaTeX format for writing academic research papers, and although I was initially apprehensive to venture it, the ease with which I was able to format my thesis made it well worth the effort.

The magnitude of completing this thesis would not have been possible without the selfless support and sacrifice of my wife, Sharon, who took the time to nurture our two children, Rianne and Rayden, during this one-year stay in the United States, while at the same time, allowing me to concentrate on pursuing my academic achievements. Their youthful and chirpy presence in the family served to lift the stressful mood off my shoulders as I continued on my studies and thesis inquest, often into the wee hours of the day.

I am also grateful for the support rendered to me by my fellow aspiring mathematicians, Scott Warnke, Karoline Hood, Ryan Miller, and Zack Lukens, with whom I had the privilege to not only share an office, but also to spar mathematically with. The good times that we had during Thanksgiving and various other festive activities will no doubt be lasting wonderful memories.

Last but not least, I would like to give a special shout-out to Associate Professor Bard

Mansager, my academic advisor in the Department of Applied Mathematics. Bard was the one who reassured me that the Math Department will take good care of me during my time in NPS, and I am indeed honored to be part of this wonderful family during my short stint here.

Looking back, this one year has passed by in the blink of an eye. The time spent here in Monterey and NPS had been nothing short of mesmerizing and fantastic. For friends and colleagues who I am unable to thank here, I offer my sincerest apologies, but nevertheless would like to thank them for offering me advice, guidance, and domain expertise during this arduous journey.

CHAPTER 1:
Introduction to Secret Sharing

Imagine you have been given the task of finding out the average salary of a room full of N highly successful individuals. The obvious way is to sum up all the individuals' salaries and average the summation over the total number of people in the room. The problem is that none of the individuals want to disclose their monthly income because such figures are highly confidential and sensitive.

Here is a viable solution. Have Person A come up with a random number, say $[\alpha]$, and Person A is to add his or her own salary to $[\alpha]$. This new value is to be passed on to Person B, who will then add his or her own salary to the new value received from Person A. Now, Person B does not know how much Person A's salary is, since he or she does not know what random number $[\alpha]$ Person A has chosen.

The process repeats itself until the last person in the room, Person N, receives the new value from the second-to-last person, Person $N-1$. Person N continues to add on his or her salary, and the final value, say $[\beta]$, is then passed back to Person A. At this stage, Person A simply needs to deduct $[\alpha]$ from $[\beta]$ (since only he or she knows what $[\alpha]$ is), and average this sub-total over the number of people in the room, N. In this way, the average salary in the room can be obtained, without any person revealing his or her income.

The value of $[\alpha]$ is critical in this instance, as it provides a gateway to gather information from multiple sources without each source revealing unwanted information that should otherwise remain secret. For example, if any person in the room other than Person A would know the value of $[\alpha]$, then he or she could find out Person A's income by simply providing the information to Person B and having Person B perform the arithmetic.

Consider another secret sharing example. A bank vault in a highly secured bank requires three keys to open. The key holders are already designated to be two of the bank's top hierarchy. But strict financial regulations state that no one person should be in total possession of the three keys, for fear of corruption. The logical partition would be to split the keys between these two personnel. With both needing equal authority over the safekeeping of

the bank vault, this constitutes a conundrum.

The *two-man rule* states that all actions and access requires the presence of two authorized people at all times. In the bank vault secret sharing example, the logical way to follow this rule is to let Person A hold on to Key 1 and Key 2, and Person B hold on to Key 2 and Key 3. In this way, no single person can open the bank vault (since the vault needs three keys), and both authorized persons (given equal authority by holding two keys each) need to be present in order to open the vault.

The methodology of sharing secrets (or, splitting secrets) was independently invented by Adi Shamir [1] and George Blakley [2] in 1979. Being one of the most well-known and dominant secret sharing schemes, in this thesis, Shamir's Secret Sharing Scheme [1] is mainly analysed.

1.1 Shamir's Secret Sharing Scheme

Shamir's Secret Sharing Scheme comprises the general distribution of shares to various n participants, where each participant is holding on to a unique share. In order to re-construct the secret, some or all of the parts are needed. Since gathering all the participants to reconstruct the secret may be impractical, the threshold scheme is thus formulated where any k parts will be sufficient to re-construct the secret. This is also known as the $\{k,n\}$ threshold scheme. If $k = n$, then all participants are required in order to reveal the secret.

In general, the secret S is divided into n pieces of data $S_1, S_2, \ldots, S_n$, in such a way that

- k or more S_i shares is enough to piece together the secret.
- $k-1$ or fewer S_i shares is not enough to determine the secret (other than trying all possibilities).

1.1.1 Secret Sharing Example using a Quadratic Polynomial

Assume that the secret value to be kept is $4,321$ (i.e., $S = 4,321$), and the threshold scheme is to be set as $\{3,7\}$ (i.e., any subset of three shares out of the possible seven shares is sufficient to construct the secret). Randomly, $(k-1)$ integers are picked to construct the $(k-1)^{th}$ degree polynomial:

$$a_1 = 69, a_2 = 213.$$

The polynomial to produce the required number of secret shares is thus constructed to be

$$f(x) = 4321 + 69x + 213x^2. \tag{1.1}$$

Since there are seven shares, seven points are then constructed from Eqn. (1.1). These seven points are as follows:

Table 1.1: Seven Points Constructed from a Quadratic Polynomial

x	$y = f(x)$
1	4603
2	5311
3	6445
4	8005
5	9991
6	12403
7	15241

In order to reconstruct the secret, any three shares are sufficient. Consider the following three random points $P_0 = (x_0, y_0) = (1, 4603)$; $P_1 = (x_1, y_1) = (3, 6445)$; and $P_2 = (x_2, y_2) = (5, 9991)$. The theory of Lagrange polynomial interpolation is used to reconstruct the secret:

$$\begin{aligned}
l_0(x) &= \frac{x-x_1}{x_0-x_1}.\frac{x-x_2}{x_0-x_2} = \frac{x-3}{1-3}.\frac{x-5}{1-5} = \frac{1}{8}(x-3)(x-5), \\
l_1(x) &= \frac{x-x_0}{x_1-x_0}.\frac{x-x_2}{x_1-x_2} = \frac{x-1}{3-1}.\frac{x-5}{3-5} = -\frac{1}{4}(x-1)(x-5), \\
l_2(x) &= \frac{x-x_0}{x_2-x_0}.\frac{x-x_1}{x_2-x_1} = \frac{x-1}{5-1}.\frac{x-3}{5-3} = \frac{1}{8}(x-1)(x-3).
\end{aligned}$$

By Lagrange interpolation, the polynomial is recovered by using

$$\begin{aligned} f(x) &= \sum_{i=0}^{2} l_i(x) \cdot y_i \\ &= [\frac{1}{8}(x-3)(x-5)] \times 4603 + [-\frac{1}{4}(x-1)(x-5)] \times 6445 + [\frac{1}{8}(x-1)(x-3)] \times 9991, \\ &= 4321 + 69x + 213x^2. \end{aligned}$$

The constant coefficient (or a_0) found to be equal to the initial secret value, and the secret reconstruction is complete.

1.1.2 Secret Sharing Example Using a Cubic Polynomial

If a minimum of four shares were desired for the secret reconstruction for a $\{4,7\}$ threshold scheme, then a cubic polynomial will be formed. Consider the following example:

$$S = 36, a_1 = 6, a_2 = 4, a_3 = 2.$$

The polynomial is now constructed as

$$g(x) = 36 + 6x + 4x^2 + 2x^3.$$

The seven points constructed from $g(x)$ are as follows:

Table 1.2: Seven Points Constructed from a Cubic Polynomial

x	$y = g(x)$
1	48
2	80
3	144
4	252
5	416
6	648
7	960

Since four shares are required, consider the following four random points $P_0 = (x_0, y_0) = (1,48)$; $P_1 = (x_1, y_1) = (3,144)$; $P_2 = (x_2, y_2) = (5,416)$; and $P_3 = (x_3, y_3) = (7,960)$.

Lagrange interpolation is applied and the following is obtained:

$$
\begin{aligned}
l_0(x) &= \frac{x-x_1}{x_0-x_1}.\frac{x-x_2}{x_0-x_2}.\frac{x-x_3}{x_0-x_3} = \frac{x-3}{1-3}.\frac{x-5}{1-5}.\frac{x-7}{1-7} = -\frac{1}{48}(x-3)(x-5)(x-7),\\
l_1(x) &= \frac{x-x_0}{x_1-x_0}.\frac{x-x_2}{x_1-x_2}.\frac{x-x_3}{x_1-x_3} = \frac{x-1}{3-1}.\frac{x-5}{3-5}.\frac{x-7}{3-7} = \frac{1}{16}(x-1)(x-5)(x-7),\\
l_2(x) &= \frac{x-x_0}{x_2-x_0}.\frac{x-x_1}{x_2-x_1}.\frac{x-x_3}{x_2-x_3} = \frac{x-1}{5-1}.\frac{x-3}{5-3}.\frac{x-7}{5-7} = -\frac{1}{16}(x-1)(x-3)(x-7),\\
l_3(x) &= \frac{x-x_0}{x_3-x_0}.\frac{x-x_1}{x_3-x_1}.\frac{x-x_2}{x_3-x_2} = \frac{x-1}{7-1}.\frac{x-3}{7-3}.\frac{x-5}{7-5} = \frac{1}{48}(x-1)(x-3)(x-5).
\end{aligned}
$$

The polynomial is then recovered by using

$$
\begin{aligned}
g(x) &= \sum_{i=0}^{3} l_i(x)\cdot y_i\\
&= [-\frac{1}{48}(x-3)(x-5)(x-7))]\times 48+\\
&\quad [\frac{1}{16}(x-1)(x-5)(x-7)]\times 144+\\
&\quad [-\frac{1}{16}(x-1)(x-3)(x-7)]\times 416+\\
&\quad [\frac{1}{48}(x-1)(x-3)(x-5)]\times 960,\\
&= 36+6x+4x^2+2x^3.
\end{aligned}
$$

The constant coefficient (or a_0) is equal to the initial secret value, and thus the secret reconstruction is complete.

In general, in order to implement the $\{k,n\}$ threshold scheme, a polynomial of degree $k-1$ is required. The degree $k-1$ polynomial will have k coefficients that can be recovered by any system with any k equations.

1.2 Formal Definitions for Abstract Algebra

In order to aid in the analysis of Shamir's Secret Sharing Scheme (SSSS), and to simplify the polynomials used in the scheme, it is necessary to define some basic theorems on linear and abstract algebra. Much of the information can be obtained from related mathematical texts, such as John B. Fraleigh's *A First Course in Abstract Algebra* [3]. The related definitions from the text are extracted and presented here.

1.2.1 Abstract Algebra — Groups, Rings, Fields, Finite Fields

Definition 1.2.1. [3, pp. 37–39] A **group** $< G, * >$ is a set G, closed under a binary operation *, such that the following axioms are satisfied:
$\mathscr{G}_1$: For all $a, b, c \in G$, the **associativity** of *, $(a * b) * c = a * (b * c)$ holds.
$\mathscr{G}_2$: There is an element e in G such that for all $x \in G$, $e * x = x * e = x$. This is also known as the **identity element** e for *.
$\mathscr{G}_3$: Corresponding to each $a \in G$, there is an element $a' \in G$ such that $a * a' = a' * a = e$. This means that the **inverse** of a exists. A group is **abelian** if its binary operation is commutative.

Definition 1.2.2. [3, pp. 167] The most general algebraic structure, **ring** $< R, +, \cdot >$, is a set R together with two binary operations $+$ and $\cdot$, namely addition and multiplication, defined on R such that the following axioms are satisfied:
$\mathscr{R}_1$: $< R, + >$ is an abelian group.
$\mathscr{R}_2$: $< R, \cdot >$ is associative, or monoid.
$\mathscr{R}_3$: For all $a, b, c \in R$, the **left distributive law** $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$, and the **right distributive law** $(a + b) \cdot c = (a \cdot c) + (b \cdot c)$ hold.

Definition 1.2.3. [3, pp. 172–174] By extension, a **field** $< F, +, \cdot >$, is a set F with two binary operations, namely addition and multiplication, defined on F, and satisfies the following axioms:
$\mathscr{F}_1$: $< F, + >$ is an abelian group.
$\mathscr{F}_2$: $< F^*, \cdot >$ is an abelian group.
$\mathscr{F}_3$: For all $a, b, c \in F$, the **distributive law** $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$ holds.

Definition 1.2.4. [3, pp. 300] A **finite field** is thus a field with a finite number of elements. It is known, and easy to show that, for every prime p, and positive integer n, there is exactly

one finite field (up to isomorphism) of order p^n. [Usually], this field [denoted] $GF(p^n)$ is referred to as the **Galois field of order** p^n.

In general, since the identity condition is required to be different for addition and multiplication, there must be at least two elements in every field. Some common examples include $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, that is, the rational numbers, the real numbers, and the complex numbers, respectively. It must be noted that $\mathbb{Z}$, the integers, form only a ring. Thus, in this thesis, both the integer ring $\mathbb{Z}$, and the prime field $\mathbb{Z}_p$, where p is a prime number, are often referenced; the latter is mainly due to the unique properties of prime numbers.

1.3 Research Objective

The purpose of this thesis is to analyse Shamir's Secret Sharing Scheme and to identify weaknesses and potential improvements, and to build upon them to discuss the side-channel effects on the Advanced Encryption Standard (AES).

The following questions are asked:

- Can pre-existing conjectures and theorems be used to improve and/or weaken the security and simplify the computational complexity of the present secret sharing scheme?
- Can the improvements to the current secret sharing scheme prove to be beneficial in strengthening/weakening AES encryption, such as side-channel analysis?

THIS PAGE INTENTIONALLY LEFT BLANK

CHAPTER 2:
Analysis of Shamir's Secret Sharing Scheme

2.1 The Importance of the Dealer

For a $\{k,n\}$ threshold scheme, the dealer computes the degree $(k-1)$ polynomial and embeds the secret within the polynomial. The dealer also has to provide the public values by computing the required outputs using certain inputs. The generated polynomial is of the form

$$f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_{k-1} x^{k-1}, \tag{2.1}$$

where a_0 is the secret and a_i, $1 \leq i \leq k-1$, are chosen randomly.

2.2 Order of Difficulty in Reconstructing the Secret

In this thesis, it is assumed that the Lagrange interpolation to reconstruct the secret is done over an integer ring. Performing arithmetic over the integer field $\mathbb{Z}_p$ will, however, improve on the computational efficiency, as is discussed later. For example, if the Lagrange interpolation is done over the residue field $\mathbb{Z}_p$ (that is, over modulo p), then the order of computational complexity is $O(p^k)$.

2.3 Simplifying Secret Sharing Polynomials — Potential Weakness?

The initial degree $(k-1)$ polynomial $f(x)$ is created by the dealer. There is no way to retrieve the secret unless at least k participants come together to reconstruct the secret using Lagrange interpolation. A viable idea to improve the simplicity of the polynomial is to introduce a composition of another function that may be easier to dissect with existing mathematical tools.

Consider the following manipulation of the polynomial functions:

Let $f(x) = h(x) \circ g(x)$, where
$f(x)$ is the degree $(k-1)$ polynomial generated by the dealer;

$h(x)$ is the desired final simplified polynomial of the form $(x-\alpha)^k - b_0$; and
$g(x)$ is a linear function to be applied to $h(x)$ to form the original polynomial.

Consider first the composite function $g(x) = x + \alpha$, and the following is obtained. First, it is desired to simplify $f(x)$ to be in the form of $f(x) = x^k - b_0$, for some coefficients in the dealer-generated polynomial. Hence, $f(x) = h(g(x)) = h(x+\alpha) = x^k - b_0$. Therefore, $h(x) = f(x-\alpha)$, and so,

$$\begin{aligned} h(x) &= f(x-\alpha) = (x-\alpha)^k - b_0, \\ &= \left[x^k + \binom{k}{1}x^{k-1}(-\alpha)^1 + \binom{k}{2}x^{k-2}(-\alpha)^2 + \cdots + (-\alpha)^k\right] - b_0, \\ &= \left[x^k + \sum_{i=1}^{k-1} c_i x^{k-i} + (-\alpha)^k\right] - b_0, \end{aligned} \tag{2.2}$$

where $c_i = \binom{k}{i}(-\alpha)^i$.

It is clear that the values of c_i correspond to the coefficients of the original dealer-generated polynomial.

If the value $x = 0$ is applied into the final form of Eqn. (2.2), the output will correspond to the hidden secret, since it is known that the secret is the value of a_0 in the original polynomial generated by the dealer in Eqn. (2.1).

Therefore, from Eqns. (2.1) and (2.2), the secret can be derived as the coefficient without any x terms:

$$Secret = a_0 = (-\alpha)^k - b_0. \tag{2.3}$$

If the values of α and b_0 are known, then the secret is unravelled. The challenge then, is to find the values of α and b_0, if they are unknown, in order to reconstruct the secret.

2.4 Finding the Values of α and b_0

If the Lagrange interpolation is performed modulo p, then finding the value of α is of order $O(p^k)$, and likewise for the finding of b_0. Therefore, if both α and b_0 are unknown, the whole problem of finding both values escalates to order $O(p^k \times p^k) = O(p^{2k})$.

The famous Pillai's conjecture, and various other conditions related to the conjecture, are used to simplify the range of values of both α and b_0.

THIS PAGE INTENTIONALLY LEFT BLANK

CHAPTER 3:
Applying Pillai's Conjecture to Secret Sharing Schemes

3.1 Pillai's Conjecture (General)

Herschfeld (1936) [4] showed that the equation $3^x - 2^y = c$, for $|c|$ sufficiently large, has at most a solution in positive integers x, y. In the same year, Pillai extended this result, by considering the exponential Diophantine equation

$$a^x - b^y = c,$$

and proved that there exists a finite number of positive integer solutions $(a, b, x, y \in \mathbb{Z})$, with $x \geq 2$ and $y \geq 2$, to this Diophantine equation [5], provided $|c| > c_0(a,b)$, for some constant $c_0(a,b)$, which unfortunately is ineffectively computable. Pillai conjectured that $c_0(3,2) = 13$, this being proved in 1982 by Stroeker and Tijdeman [6], using methods based on Baker's linear forms in logarithms. The general Pillai's conjecture (see Conjecture 3.1.1, following) that gives an estimate for c_0 will be mostly used to find a weakness in Shamir's Secret Sharing Scheme. The quantitative refinement of the already mentioned (general) Pillai's conjecture is also discussed by Waldschmidt [5].

Conjecture 3.1.1. For any $\varepsilon > 0$, there exists a constant $\kappa(\varepsilon) > 0$, such that, for any positive integers $a, b, x \geq 2, y \geq 2$, with $a^x \neq b^y$, then

$$|a^x - b^y| \geq \kappa(\varepsilon) \times max(a^x, b^y)^{(1-\frac{1}{x}-\frac{1}{y}-\varepsilon)}. \tag{3.1}$$

3.2 Fermat-Catalan Conjecture

This conjecture was proposed based upon both Fermat's Last Theorem, and Catalan's conjecture. In 1995, Richard Taylor and Andrew Wiles [7] co-published an article thereby proving Fermat's Last Theorem.

Theorem 3.2.1. Fermat's Last Theorem states that for any integer n that is greater than two,

there do not exist any three (strictly) positive integers a, b, and c that satisfy the equation $a^n + b^n = c^n$.

Referencing Conjecture 3.1.1, in 2002, Mihăilescu [8] proved Catalan's conjecture.

Conjecture 3.2.1 (Mihăilescu Theorem)**.** The only solutions to the equation $a^x - b^y = 1$ are 3^2 and 2^3.

The Fermat–Catalan conjecture combines the ideas of Fermat's Last Theorem and Catalan's conjecture. In 1995, Darmon and Granville [9] proved the conjecture.

Conjecture 3.2.2. The equation $a^m + b^n = c^k$ has a finite number of solutions that satisfy the inequality $\frac{1}{m} + \frac{1}{n} + \frac{1}{k} < 1$.

Definition 3.2.1. Two integers a and b are coprime if the only positive integer that evenly divides both a and b is 1, that is, if their greatest common divisor, $gcd(a,b) = 1$.

3.3 Motivation

By Theorem 3.2.1 and Conjecture 3.2.2, it is inferred by Waldschmidt [5] that, $\forall \varepsilon > 0$, $\exists \kappa(\varepsilon) > 0$ such that

$$a^x - b^y = c \Rightarrow |a^x - b^y| \geq \kappa(\varepsilon) \times max(a^x, b^y)^{1-\frac{1}{x}-\frac{1}{y}-\varepsilon}. \tag{3.2}$$

From Catalan's conjecture, the equation $a^x - b^y$ yields a constant c. This relationship is used in conjunction with the Fermat-Catalan conjecture in Definition 3.2.2 to improve the efficiency in recovering the secret in secret sharing schemes. The motivation is thus to streamline the ranges between a^x and b^y such that the maximum value between these two components can be easily found. Coupled with the relationship that the power $(1 - \frac{1}{x} - \frac{1}{y} - \varepsilon)$ is always < 1, the final value of $|a^x - b^y|$ will be even smaller. This will greatly reduce the computational complexity involved.

Applications of this relationship are further discussed in the next chapter.

CHAPTER 4:
Exploring Secret Sharing

4.1 Applying Fermat-Catalan Conjecture to Secret Sharing Scheme

Consider the following analysis for the $\{k+1,n\}$ threshold scheme.

Let $f(x)$ be defined as the degree k polynomial generated by the dealer:

$$f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_k x^k, \tag{4.1}$$

where a_0 is the secret to be shared.

Assume that there exists $\alpha \in \mathbb{Z}_p$, such that $h(x) = f(x-\alpha) = x^k - b_0$ (consider that the dealer-generated polynomial is monic — the case of non-monic polynomials can still be dealt with, but one needs at least three shares to be known). In this case, the leading coefficient a_k of the highest degree term x^k is 1.

Let $f(x_1), f(x_2), ..., f(x_n)$ be defined as the shares to be handed out, where $f(x_i) = y_i$. If $f(x_1), f(x_2), \ldots, f(x_n)$ are known, then the following can be inferred:

$$(x_1 - \alpha)^k - b_0 = y_1,$$

$$(x_2 - \alpha)^k - b_0 = y_2,$$

$$\ldots\ldots\ldots\ldots$$

$$(x_n - \alpha)^k - b_0 = y_n.$$

It must be noted that any set of $k+1$ shares is sufficient to recover the secret, even though a total of n shares are generated. This is the core essence of Shamir's Secret Sharing Scheme. However, under the assumption, it is possible to recover the secret with significantly fewer shares, in this case, two.

Taking the difference of any two equations, this leads to the generalized equation where b_0 is eliminated:

$$(x_i - \alpha)^k - (x_j - \alpha)^k = y_i - y_j, \tag{4.2}$$

where $1 \leq i < j \leq n$.

Note that the right-hand side is known since those are the outputs generated and distributed by the dealer to various participants.

Referencing the extension of Pillai's Diophantine equation in Eqn. (3.1) leads to

$$|a^x - b^y| \geq \kappa(\varepsilon) \times max(a^x, b^y)^{1-\frac{1}{x}-\frac{1}{y}-\varepsilon}.$$

Replacing a^x with $(x_i - \alpha)^x$, and b^y with $(x_j - \alpha)^y$ leads to

$$|(x_i - \alpha)^x - (x_j - \alpha)^y| \geq \kappa(\varepsilon) \times max(|x_i - \alpha|^k, |x_j - \alpha|^k)^{1-\frac{1}{x}-\frac{1}{y}-\varepsilon}.$$

For the purpose of secret sharing, let $x = y = k$, which results in

$$|(x_i - \alpha)^k - (x_j - \alpha)^k| \geq \kappa(\varepsilon) \times max(|x_i - \alpha|^k, |x_j - \alpha|^k)^{1-\frac{1}{k}-\frac{1}{k}-\varepsilon}.$$

Using Eqn. (4.2) in the left-hand side of the above inequality, it is finally deduced that $\forall \varepsilon > 0$, $\exists \kappa(\varepsilon) > 0$, such that

$$|y_i - y_j| \geq \kappa(\varepsilon) \times max(|x_i - \alpha|^k, |x_j - \alpha|^k)^{1-\frac{2}{k}-\varepsilon}. \tag{4.3}$$

4.2 Significance of $\kappa(\varepsilon)$

In 1970, Marshall Hall, Jr. [10], proposed to remove the value of $\kappa(\varepsilon)$ for the quantitative case when $x = 3$ and $y = 2$.

Conjecture 4.2.1. There exists an absolute constant $C > 0$ such that, for any pair of (x, y)

of positive integers satisfying $x^3 \neq y^2$,

$$|x^3 - y^2| > C \times max(x^3, y^2)^{(1-\frac{1}{2}-\frac{1}{3})}.$$

This is also known as Hall's conjecture, which will be drawn upon to further simplify the problem (for example, it is further believed that $C \leq 0.96598\ldots$).

Presumably, $\kappa(\varepsilon)$ is computable and quite small (e.g., see Bennett's work on Pillai's conjecture [11], in particular when $|a-b| = 1$), so for this purpose, it is possible, for example, to assume ε to be strictly less than $1 - \frac{2}{k}$, in order to find the *finite* bounds for $|x_i - \alpha|, |x_j - \alpha|$ (see the analysis in the following sections) .

4.3 Forming the Inequalities to Find the Bounds for Computing the Value of α

Focusing on the right-hand side of Eqn. (4.3), and assuming $\kappa(\varepsilon) = 1$, the following arithmetic is performed on one of the terms:

$$(|x_j - \alpha|^k)^{1-\frac{2}{k}-\varepsilon} = (|x_j - \alpha|^k)^{\frac{k-2-k\varepsilon}{k}} = (|x_j - \alpha|)^{k-2-k\varepsilon}. \tag{4.4}$$

From Inequality (4.3), it is inferred that

$$|x_j - \alpha|^{k-2-k\varepsilon} \leq |y_i - y_j|,$$

$$|x_j - \alpha| \leq |y_i - y_j|^{\frac{1}{k-2-k\varepsilon}}. \tag{4.5}$$

With this inequality, the complexity of the problem is now significantly reduced. It is now reduced to simply finding the values of α from Eqn. (4.5), whereby the values of x_j, y_i, y_j, k, and ε are known, and are small enough to compute.

The order of computational difficulty is now reduced significantly from the initial order of $O(p^k)$, or $O(p^{2k})$ if there are two unknowns.

Applying (an extension of) Hall's conjecture, whereby the value of ε is assumed to be 0,

Eqn. (4.5) now reduces further to

$$(|x_j - \alpha|) \leq |y_i - y_j|^{\frac{1}{k-2}}. \tag{4.6}$$

4.4 Dissecting the Inequalities

It was assumed that $\exists\alpha$ such that $h(x) = f(x-\alpha) = x^k - b_0$, for certain cases of the polynomial form that was generated by the dealer.

Since $f(x-\alpha) = x^k - b_0$, this can be rewritten as $f(x) = (x+\alpha)^k - b_0$.

In a $\{k+1, n\}$ threshold scheme, n shares are generated, namely $(x_1, y_1), (x_2, y_2), \cdots, (x_n, y_n)$, where $y_i = f(x_i)$, for $1 \leq i \leq n$.

Consider the case where it is sufficient to pool together two known pairs (shares). Therefore, the following is derived:

$$y_1 = (x_1 + \alpha)^k - b_0,$$

$$y_2 = (x_2 + \alpha)^k - b_0,$$

$$y_1 - y_2 = (x_1 + \alpha)^k - (x_2 + \alpha)^k,$$

or,

$$y_2 - y_1 = (x_2 + \alpha)^k - (x_1 + \alpha)^k.$$

Solving for the value of α is not trivial for large values of k, especially if k is prime. A prime k, however, will allow performing finite field arithmetic to reduce the bounds of α, which is discussed later in greater detail.

For simplicity's sake, the labels $\mathbb{A} := x_1 + \alpha$, and $\mathbb{B} := x_2 + \alpha$ are applied, hence $\mathbb{A}^k = (x_1 + \alpha)^k$, and $\mathbb{B}^k = (x_2 + \alpha)^k$. In addition, it is clear that $(\mathbb{A} - \mathbb{B}) = (x_1 - x_2)$.

The following identity is used

$$(\mathbb{A}^k - \mathbb{B}^k) = (\mathbb{A} - \mathbb{B}) \times (\mathbb{A}^{k-1} + \mathbb{A}^{k-2}\mathbb{B} + \cdots + \mathbb{A}\mathbb{B}^{k-2} + \mathbb{B}^{k-1}),$$

to infer

$$(y_1 - y_2) = (x_1 - x_2) \times (\mathbb{A}^{k-1} + \mathbb{A}^{k-2}\mathbb{B} + \cdots + \mathbb{A}\mathbb{B}^{k-2} + \mathbb{B}^{k-1}),$$

$$\frac{y_1 - y_2}{x_1 - x_2} = (\mathbb{A}^{k-1} + \mathbb{A}^{k-2}\mathbb{B} + \cdots + \mathbb{A}\mathbb{B}^{k-2} + \mathbb{B}^{k-1}).$$

It is obvious that the following inequality holds:

$$(|\mathbb{A}|^{k-1} + |\mathbb{A}|^{k-2}|\mathbb{B}| + \cdots + |\mathbb{A}||\mathbb{B}|^{k-2} + |\mathbb{B}|^{k-1}) \geq max(|\mathbb{A}|^{k-1}, |\mathbb{B}|^{k-1}). \tag{4.7}$$

Eqn. (4.7) is now used to consider all possible cases of polarity for the values of $\mathbb{A}$, $\mathbb{B}$, and parity for the values of k. Note that since k is a known positive value, and ≥ 2, it is necessary to only consider cases where k is either even or odd. For the case where $k = 2$, it is easy to find α since $y_1 - y_2$ is just the difference of squares.

4.4.1 Case 1 — $[\mathbb{A} > 0, \mathbb{B} > 0]$

Without loss of generality (WLOG), assume that $\mathbb{A} > \mathbb{B}$ (equality cases are impossible). Therefore, the following is obtained:

$$\frac{y_1 - y_2}{x_1 - x_2} = (\mathbb{A}^{k-1} + \mathbb{A}^{k-2}\mathbb{B} + \cdots + \mathbb{A}\mathbb{B}^{k-2} + \mathbb{B}^{k-1}),$$

$$\frac{y_1 - y_2}{x_1 - x_2} \geq max(|\mathbb{A}|^{k-1}, |\mathbb{B}|^{k-1}) = |\mathbb{A}|^{k-1},$$

$$\frac{y_1 - y_2}{x_1 - x_2} \geq (|x_1 + \alpha|)^{k-1},$$

$$(\frac{y_1 - y_2}{x_1 - x_2})^{\frac{1}{k-1}} \geq (|x_1 + \alpha|),$$

$$-(\frac{y_1 - y_2}{x_1 - x_2})^{\frac{1}{k-1}} - x_1 \leq \alpha \leq (\frac{y_1 - y_2}{x_1 - x_2})^{\frac{1}{k-1}} - x_1.$$

With the known values of x_1, x_2, y_1, y_2, and k, respectively, both lower bounds and upper bounds of α are found.

For the case where both $\mathbb{A}$ and $\mathbb{B}$ are positive, the parity of k does not matter since applying the same exponential power to both $\mathbb{A}$ and $\mathbb{B}$ does not change the comparison between them. To be more encompassing, it is therefore necessary to consider different parity cases

of the value of k, along with the polarities of both $\mathbb{A}$ and $\mathbb{B}$. Instead of always assuming that $\mathbb{A} > \mathbb{B}$ for all cases (since the value of α is unknown at this point), the polarity of the denominator $(x_1 - x_2)$ is also included in each individual case analysis.

4.4.2 Case 2 — [$\mathbb{A} < 0, \mathbb{B} > 0$] [$k$ odd]

With these constraints, and since k is odd,

$$\begin{aligned} y_2 - y_1 &= \mathbb{B}^k - \mathbb{A}^k, \\ &= \mathbb{B}^k + |\mathbb{A}|^k, \\ &\geq max(\mathbb{B}^k, |\mathbb{A}|^k). \end{aligned}$$

Again, WLOG, consider the case where $\mathbb{B}^k > |\mathbb{A}|^k$:

$$y_2 - y_1 \geq max(\mathbb{B}^k, |\mathbb{A}|^k) \geq \mathbb{B}^k,$$

$$(y_2 - y_1)^{\frac{1}{k}} \geq \mathbb{B},$$

$$(y_2 - y_1)^{\frac{1}{k}} \geq |x_2 + \alpha|,$$

$$-(y_2 - y_1)^{\frac{1}{k}} - x_2 \leq \alpha \leq (y_2 - y_1)^{\frac{1}{k}} - x_2.$$

With this, the lower and upper bounds of α can be found easily. It is impractical to reduce $\mathbb{B}^k + |\mathbb{A}|^k$ according to the identity that was mentioned earlier, as it would be indeterminable whether $\mathbb{B} + |\mathbb{A}|$ would be a positive value, and hence the maximum inequality would not apply.

4.4.3 Case 3 — [$\mathbb{A} > 0, \mathbb{B} < 0$] [$k$ odd]

In this case, since k is odd, the following is obtained:

$$y_2 - y_1 = \mathbb{B}^k - \mathbb{A}^k,$$

$$y_1 - y_2 = \mathbb{A}^k - \mathbb{B}^k = \mathbb{A}^k + |\mathbb{B}|^k \geq |\mathbb{A}|^k,$$

$$(y_1 - y_2)^{\frac{1}{k}} \geq |\mathbb{A}|,$$

$$(y_1 - y_2)^{\frac{1}{k}} \geq |x_1 + \alpha|,$$
$$-(y_1 - y_2)^{\frac{1}{k}} - x_1 \leq \alpha \leq (y_1 - y_2)^{\frac{1}{k}} - x_1.$$

This essentially gives similar results as Case 2, except for the value interchange between y_1 and y_2, and x_1 being used as the variable difference in this case.

4.4.4 Case 4 — [$\mathbb{A}, \mathbb{B} < 0$] [$k$ odd]

Consider the last case of odd k, with both parameters less than 0. The following is obtained:

$$\begin{aligned} y_2 - y_1 &= \mathbb{B}^k - \mathbb{A}^k, \\ &= -|\mathbb{B}|^k + |\mathbb{A}|^k, \\ &= |\mathbb{A}|^k - |\mathbb{B}|^k. \end{aligned}$$

WLOG, assume that $|\mathbb{A}| > |\mathbb{B}|$. Therefore,

$$\begin{aligned} 0 < y_2 - y_1 &= |\mathbb{A}|^k - |\mathbb{B}|^k, \\ &= (|\mathbb{A}| - |\mathbb{B}|) \times (|\mathbb{A}|^{k-1} + |\mathbb{A}|^{k-2}|\mathbb{B}| + \cdots + |\mathbb{B}|^{k-1}), \\ &= (x_1 - x_2) \times (|\mathbb{A}|^{k-1} + |\mathbb{A}|^{k-2}|\mathbb{B}| + \cdots + |\mathbb{B}|^{k-1}), \\ &\geq |\mathbb{A}|^{k-1}. \end{aligned}$$

Thus,

$$y_2 - y_1 \geq |\mathbb{A}|^{k-1},$$
$$(y_2 - y_1)^{\frac{1}{k-1}} \geq |\mathbb{A}|,$$
$$(y_2 - y_1)^{\frac{1}{k-1}} \geq |x_1 + \alpha|,$$
$$-(y_2 - y_1)^{\frac{1}{k-1}} - x_1 \leq \alpha \leq (y_2 - y_1)^{\frac{1}{k-1}} - x_1.$$

Case 4 now concludes the analysis for odd values of k. The analysis focus is now shifted to even values of k.

4.4.5 Case 5 — [$\mathbb{A} < 0, \mathbb{B} > 0$] [$k$ even]

Since k is even, the following is obtained:

$$\begin{aligned} y_2 - y_1 &= \mathbb{B}^k - \mathbb{A}^k, \\ &= \mathbb{B}^k - |\mathbb{A}|^k. \end{aligned}$$

WLOG, now assume that $\mathbb{B} > |\mathbb{A}|$. The following is obtained:

$$\begin{aligned} 0 < y_2 - y_1 &= \mathbb{B}^k - |\mathbb{A}|^k, \\ &= (\mathbb{B} - |\mathbb{A}|) \times (\mathbb{B}^{k-1} + \mathbb{B}^{k-2}|\mathbb{A}| + \cdots + |\mathbb{A}|^{k-1}), \\ &= (x_2 - x_1) \times (\mathbb{B}^{k-1} + \mathbb{B}^{k-2}|\mathbb{A}| + \cdots + |\mathbb{A}|^{k-1}), \\ &\geq |\mathbb{A}|^{k-1}. \end{aligned}$$

$$\begin{aligned} y_2 - y_1 &\geq |x_1 + \alpha|^{k-1}, \\ (y_2 - y_1)^{\frac{1}{k-1}} &\geq |x_1 + \alpha|, \\ -(y_2 - y_1)^{\frac{1}{k-1}} - x_1 \leq \alpha &\leq (y_2 - y_1)^{\frac{1}{k-1}} - x_1. \end{aligned}$$

4.4.6 Case 6 — [$\mathbb{A} > 0, \mathbb{B} < 0$] [$k$ even]

With these constraints, and k odd,

$$\begin{aligned} y_2 - y_1 &= \mathbb{B}^k - \mathbb{A}^k, \\ &= |\mathbb{B}|^k - \mathbb{A}^k. \end{aligned}$$

Now, WLOG, assume that $|\mathbb{B}| > \mathbb{A}$. Therefore,

$$\begin{aligned} 0 < y_2 - y_1 &= |\mathbb{B}|^k - \mathbb{A}^k, \\ &= (|\mathbb{B}| - \mathbb{A}) \times (|\mathbb{B}|^{k-1} + |\mathbb{B}|^{k-2}\mathbb{A} + \cdots + \mathbb{A}^{k-1}), \\ &= (x_2 - x_1) \times (|\mathbb{B}|^{k-1} + |\mathbb{B}|^{k-2}\mathbb{A} + \cdots + \mathbb{A}^{k-1}), \\ &\geq |\mathbb{B}|^{k-1}. \end{aligned}$$

$$y_2 - y_1 \geq |\mathbb{B}|^{k-1},$$
$$y_2 - y_1 \geq |x_2 + \alpha|^{k-1},$$
$$(y_2 - y_1)^{\frac{1}{k-1}} \geq |x_2 + \alpha|,$$
$$-(y_2 - y_1)^{\frac{1}{k-1}} - x_2 \leq \alpha \leq (y_2 - y_1)^{\frac{1}{k-1}} - x_2.$$

4.4.7 Case 7 — [$\mathbb{A}, \mathbb{B} < 0$] [$k$ even]

The last case for even k, with these constraints, are as follows:

$$\begin{aligned} y_2 - y_1 &= \mathbb{B}^k - \mathbb{A}^k, \\ &= |\mathbb{B}|^k - |\mathbb{A}|^k. \end{aligned}$$

At this point, WLOG, assume that $|\mathbb{B}| > |\mathbb{A}|$. Therefore,

$$\begin{aligned} 0 < y_2 - y_1 &= |\mathbb{B}|^k - |\mathbb{A}|^k, \\ &= (|\mathbb{B}| - |\mathbb{A}|) \times (|\mathbb{B}|^{k-1} + |\mathbb{B}|^{k-2}|\mathbb{A}| + \cdots + |\mathbb{A}|^{k-1}), \\ &= (x_2 - x_1) \times (|\mathbb{B}|^{k-1} + |\mathbb{B}|^{k-2}|\mathbb{A}| + \cdots + |\mathbb{A}|^{k-1}), \\ &\geq |\mathbb{B}|^{k-1}. \end{aligned}$$

This will produce the same results as Case 6, where the lower and upper bounds are constrained by

$$y_2 - y_1 \geq |\mathbb{B}|^{k-1},$$
$$y_2 - y_1 \geq |x_2 + \alpha|^{k-1},$$
$$(y_2 - y_1)^{\frac{1}{k-1}} \geq |x_2 + \alpha|,$$
$$-(y_2 - y_1)^{\frac{1}{k-1}} - x_2 \leq \alpha \leq (y_2 - y_1)^{\frac{1}{k-1}} - x_2.$$

4.4.8 Summary of Inequality Analysis

The results obtained from the seven cases are summarized in Table 4.1.

Table 4.1: Summary of α Boundaries

Case	Polarity of $\mathbb{A}$, $\mathbb{B}$	Parity of k	Boundaries of α
1	$\mathbb{A} > \mathbb{B} > 0$	N.A.	$-(\frac{y_1-y_2}{x_1-x_2})^{\frac{1}{k-1}} - x_1 \leq \alpha \leq (\frac{y_1-y_2}{x_1-x_2})^{\frac{1}{k-1}} - x_1$
2	$\mathbb{A} < 0, \mathbb{B} > 0, \mathbb{B}^k > \lvert\mathbb{A}\rvert^k$	Odd	$-(y_2-y_1)^{\frac{1}{k}} - x_2 \leq \alpha \leq (y_2-y_1)^{\frac{1}{k}} - x_2$
3	$\mathbb{A} > 0, \mathbb{B} < 0, \mathbb{A}^k > \lvert\mathbb{B}\rvert^k$	Odd	$-(y_1-y_2)^{\frac{1}{k}} - x_1 \leq \alpha \leq (y_1-y_2)^{\frac{1}{k}} - x_1$
4	$\mathbb{A}, \mathbb{B} < 0, \lvert\mathbb{A}\rvert > \lvert\mathbb{B}\rvert$	Odd	$-(y_2-y_1)^{\frac{1}{k-1}} - x_1 \leq \alpha \leq (y_2-y_1)^{\frac{1}{k-1}} - x_1$
5	$\mathbb{A} < 0, \mathbb{B} > 0, \mathbb{B} > \lvert\mathbb{A}\rvert$	Even	$-(y_2-y_1)^{\frac{1}{k-1}} - x_1 \leq \alpha \leq (y_2-y_1)^{\frac{1}{k-1}} - x_1$
6	$\mathbb{A} > 0, \mathbb{B} < 0, \lvert\mathbb{B}\rvert > \mathbb{A}$	Even	$-(y_2-y_1)^{\frac{1}{k-1}} - x_2 \leq \alpha \leq (y_2-y_1)^{\frac{1}{k-1}} - x_2$
7	$\mathbb{A}, \mathbb{B} < 0, \lvert\mathbb{B}\rvert > \lvert\mathbb{A}\rvert$	Even	$-(y_2-y_1)^{\frac{1}{k-1}} - x_2 \leq \alpha \leq (y_2-y_1)^{\frac{1}{k-1}} - x_2$

4.5 Analysis of Bounds

The start state to form the lower and upper bounds is to take the difference between the two y-values that were easily obtained publicly. For simpler calculations, a positive difference can be obtained by identifying the bigger component and then subtracting the smaller component from it.

It was found that both the lower and upper bounds of α are constrained by the differences in the k^{th} or $(k-1)^{th}$ root of the y-value differences and the x-variable, or vice versa, depending on the assumption of whether $\mathbb{A}^k$ or $\mathbb{B}^k$ is larger.

The initial assumption was that computation may be easier with even values of k, since even powers of positive or negative functions still produce positive results. However, it was found that the factor that limits computational efficiency is the presence of absolute values of either $\mathbb{A}$ or $\mathbb{B}$. For absolute values, there is no easy way to determine whether the actual result would be positive or negative, and hence the inequalities identity needed to be applied in order to find the bounds of α.

The crux is that as long as two shares are gathered together, the value of α can be de-

rived easily through exhaustive means. The computation is simplified even further if the differences between the y_i values found are small.

Once the value of α is found, it then remains to substitute back into the general equation $y_i = (x_i + \alpha)^k - b_0$ to determine b_0. When b_0 is found, it is trivial to find

$$f(x) = (x+\alpha)^k - b_0,$$

$$f(0) = \alpha^k - b_0 = secret.$$

4.6 Cases over Finite Field $\mathbb{Z}_p$

Computing the above arithmetic over the infinite integer ring $\mathbb{Z}$ will result in large ranges of α for which the initial polynomial can be expressed as the form $f(x) = (x+\alpha)^k - b_0$. If the above arithmetic is computed over the prime field $\mathbb{Z}_p$ instead, then the polynomial form of $f(x) = (x+\alpha)^k - b_0$ could be achieved easier as many of the coefficients would be reduced to 0 after performing modular arithmetic over the prime field. Thus, there is justifiable motivation behind the modular prime arithmetic to reduce the ranges of α to be finite and more manageable.

It was discussed earlier that the general equation $f(x) = a_0 + a_1 x + \cdots + a_k x^k$ can be expressed as

$$\begin{aligned} f(x) &= (x+\alpha)^k - b_0, \\ &= \left[x^k + \binom{k}{1} x^{(k-1)} \alpha^1 + \binom{k}{2} x^{(k-2)} \alpha^2 + \cdots + \alpha^k \right] - b_0, \\ &= \left[x^k + \sum_{i=1}^{k-1} c_i x^{(k-i)} + \alpha^k \right] - b_0. \end{aligned}$$

Computing arithmetic over $\mathbb{Z}_k$, where k is prime, gives the following result:

$$f(x) = x^k + \alpha^k - b_0.$$

And the secret is recovered as $f(0) = \alpha^k - b_0$.

4.7 Computational Example

A computational example is used to illustrate the effectiveness of the analysis.

4.7.1 Trivial Case

The following $\{3,n\}$ example has n shares and a threshold of 3 with n participants and 1 dealer. Consider the quadratic (degree $3-1=2$) polynomial generated by the dealer to be

$$f(x) = 7+4x+x^2.$$

The dealer then generates the following n shares to be released to the public, namely $(1,12),(2,19),(3,28),(4,39),(5,52),(6,67)\cdots(x_n,y_n)$. It is only necessary to find any combination of two shares to determine the value of α.

For example, if two shares, Share#1 $(2,19)$ and Share#2 $(4,39)$, are found by any individual, the general equation $f(x) = (x+\alpha)^k - b_0$ can be used as a base, and the public share values that were obtained can be substituted into the general equation:

$$GeneralEqn : f(x) = (x+\alpha)^k - b_0,$$

$$Share\#1 : 19 = (2+\alpha)^k - b_0,$$

$$Share\#2 : 39 = (4+\alpha)^k - b_0,$$

$$Share\#2 - Share\#1 : 20 = (4+\alpha)^k - (2+\alpha)^k$$

In this trivial example, if the dealer dictated that any two shares are enough to recover the secret ($k+1=3$), then finding the value of α is trivial, as one could use the difference of squares factoring. In the case of $k=2$, then

$$\begin{aligned} 20 &= (4+\alpha)^2 - (2+\alpha)^2, \\ &= (4+\alpha+2+\alpha)\times(4+\alpha-2-\alpha), \\ &= (6+2\alpha)\times(2). \end{aligned}$$

$$\therefore \alpha = 2.$$

Computing b_0,

$$\begin{aligned} b_0 &= (2+\alpha)^2 - 19, \\ &= (2+2)^2 - 19, \\ &= -3, \end{aligned}$$

which gives the secret as

$$\begin{aligned} f(0) &= (0+2)^2 - (-3), \\ &= 7. \end{aligned}$$

4.7.2 General Cases of k

Consider another numerical example, a $\{4,n\}$ threshold scheme, where the dealer-generated polynomial is

$$f(x) = x^3 + 6x^2 + 12x + 5.$$

The secret is, of course, $S = a_0 = 5$. The public shares generated, of the form (x_i, y_i), are $(1,24),(2,61),(3,122),(4,213),(5,340),\cdots,(x_n,y_n)$. Assuming that two random shares, $(1,24)$ and $(3,122)$, are obtained by an eavesdropper, and the eavesdropper decomposes the public shares into the generalized formula $y_i = (x_i+\alpha)^k - b_0$ for secret recovery, where $k = 3$,

$$24 = (1+\alpha)^3 - b_0,$$

$$122 = (3+\alpha)^3 - b_0,$$

$$\therefore (122-24) = (3+\alpha)^3 - (1+\alpha)^3. \tag{4.8}$$

This essentially gives a cubic polynomial to solve for the value of α.

Next, consider the general case for k values. For a $\{k+1,n\}$ threshold scheme, the generalized form is

$$y_i - y_j = (x_i+\alpha)^k - (x_j+\alpha)^k. \tag{4.9}$$

The problem now reduces to finding the value of α, and it can be challenging depending

on how large k is.

The analysis provided a convenient reference table in Table 4.1. In the numerical example in this section, the boundaries of α would be one of Cases 2, 3, or 4 (with k odd). Hence, α satisfies one of the following inequalities (Case 2 = Case 4):

$$-(y_2 - y_1)^{\frac{1}{k}} - x_2 \leq \alpha \leq (y_2 - y_1)^{\frac{1}{k}} - x_2,$$

or

$$-(y_1 - y_2)^{\frac{1}{k-1}} - x_1 \leq \alpha \leq (y_1 - y_2)^{\frac{1}{k-1}} - x_1.$$

Substituting all the known values from the public shares, and combining all the known information, the following is obtained:

$$\sqrt[3]{-98} - 3 \leq \alpha \leq \sqrt[3]{98} - 3.$$

Since α is an integer, the ceiling of the bounds is taken and the following is obtained:

$$-8 \leq \alpha \leq 2.$$

With these values of α, the value of b_0 can be found easily. Table 4.2 shows the values found from the iteration.

Table 4.2: Possible Secret Values

α	b_0	Secret = $f(0) = (\alpha)^k - b_0$
-8	-367	-145
-7	-240	-103
-6	-149	-67
-5	-88	-37
-4	-51	-13
-3	-32	5
-2	-25	17
-1	-24	23
0	-23	23
1	-16	17
2	3	5

It is easy to compute from Eqn. (4.8) that $\alpha = 2$, and therein lies the secret value $S = a_0 = 5$. From Table 4.2, the eavesdropper knows that the secret is one of the 11 values of $f(0)$. Hence, from an infinite number of choices (or a large finite number of choices), with just two known shares, the eavesdropper has reduced the number of secret possibilities drastically.

4.7.3 Common Factors in Polynomial Coefficients

The significance of α can be related in the generalized form of $f(x) = (x+\alpha)^k - b_0$. If the dealer-generated polynomial contains coefficients that have a common factor(s), then it is clear that α can take on the values of the common factor(s). This observation came from the fact that the generalized form of $f(x)$ is essentially a binomial expansion of the first term, and hence, the dealer needed to be careful when randomly generating the coefficients to form the polynomial for secret sharing.

The above finding leads to another observation. If the dealer generates a polynomial containing prime coefficients, then the generalized system derived from this thesis would not be applicable, as there are no common factors in prime coefficients.

4.7.4 Outcome

In a bid to continue finding ways to simplify a given polynomial to linear or monic form, the Fundamental Theorem of Algebra [3, pp. 254, 288] is referenced. The theorem states that any polynomial $f(x)$, can be factorized over the complex number field $\mathbb{C}$, as $f(x) = a_n \prod_{i=1}^{n}(x-\alpha_i)$, where n is the degree of the polynomial $f(x)$. For this analysis, by extension, this essentially means that any given dealer-generated polynomial (including non-monic polynomials) can be reduced to monic polynomials such that the generalized form of $f(x) = (x+\alpha)^k - b_0$ can be applied to reconstruct the secret from just two public shares.

It was claimed, and found, that not all monic polynomials can be reduced to the general form as proposed in this thesis. For non-monic polynomials, an eavesdropper or outsider can attempt to transform the polynomial to either a non-linear, or a monic polynomial form. Opportunities for future work of this nature are discussed in Chapter 6.

Therefore, it is important for the dealer to generate the secret polynomial with coefficients that *do not contain a common factor*. More often than not, the common factor could be the value of α for an eavesdropper or outsider whose main purpose is to reconstruct the secret *efficiently* by using only two public shares that are obtained easily.

CHAPTER 5:
Side-Channel Effect on AES

In cryptography, instead of gaining access to a cryptosystem through its algorithm, side-channel attacks are any form of attacks that are based on any viable information from the physical implementation of such a cryptosystem. Common physical parameters, including power consumption, timing codes, and operating noise level, can be used to provide a means of breaking into and crippling the cryptosystem.

This section discusses how the algorithms derived in Chapter 4 can be utilised to guard against side-channel attacks.

5.1 Cryptographic Complexity

A variation of a secret sharing scheme without the use of a cryptographic key is elaborated here.

- Encode the desired secret K_p to be an arbitrary binary string of length l.
- Generate n random binary numbers $A_1, A_2, \cdots, A_n$, whose bit lengths are equal to the size of the secret key K_p, that is, also of length l.
- Give to each participant one of $A_1, A_2, \cdots, A_{n-1}$, except for the last participant who receives the result of the following XOR function $(K_p \oplus A_1 \oplus A_2 \oplus \cdots \oplus A_{n-1})$.
- The secret can thus be recovered by gathering all of the participants' values and performing $\oplus$ operations on all of them.

This exclusive-or (XOR) variation, however, requires that all of the shares be pooled together in order to recover the secret key K_p. Compared to SSSS, this XOR method is relatively more straightforward, but offers a higher level of security since all of the participants' shares need to be present in order to recover the secret.

Blakley [2] made use of the properties of space dimensions to implement his idea of an ideal secret sharing scheme. In a three-dimensional space, three non-parallel planes will intersect at a specific point, and that point of intersection constitutes the desired secret. In a $\{3, n\}$ threshold scheme, where three shares are required to recover the secret, one can

still obtain some information about the secret. Graphically, this can be viewed as having information about the intersection of two non-parallel planes, which produces a line. The secret is thus narrowed down to an arbitrary point along the line, which can be easily recovered by substituting all the known axis values into the equation of the intersected line.

The algorithm and reasoning described in Chapter 4 made use of the fact that the secret can eventually be recovered when partial information regarding the shares is known. The principle behind forming the inequalities is to apply viable heuristics to narrow down the possibilities of unknown factors to a manageable size and then to recover the secret using exhaustive search methodologies.

5.2 Cryptographic Attacks

Chapter 2 described the importance of the dealer. Here, the importance of the dealer is amplified again during cryptographic attacks, where cyber attackers could hack into unsecured systems through side-channel attacks and steal the shares that should remain privy to only the participants. Since it would be impractical to regenerate the secret, uncompromised shares could still be updated and renewed to generate new shares for the participants. The non-updated shares that the attackers possess would become useless unless the attackers continue to obtain enough non-updated shares to reach the original threshold. The attackers would not be able to gain much information if they were to steal the updated shares since these updated shares provide only random information to the attackers. The dealer, in this scenario, possesses the ability to renew the shares, and in the process, render the non-updated shares irrelevant.

5.3 AES

In 2001, the Secretary of Commerce approved and issued the Federal Information Processing Standards Publications (FIPS PUBS) detailing the AES that can be used to protect electronic data. Essentially, AES refers to a symmetric block cipher that can encrypt (encipher) and decrypt (decipher) information. Importantly, current AES algorithms are capable of using cryptographic keys of 128, 192, and 256 bits to encrypt and decrypt data in 128-bit blocks. The current AES became effective from 2001 onwards [12]. In particular, the current AES is a block cipher that iterates ten cycles of repetitions of transformation rounds, with each of these transformation rounds involving the four stages of

AddRoundKey, *ShiftRows*, *MixColumn*, and *SubByte*, thus ensuring and enhancing the security.

5.4 Implementing AES with SSSS

Goubin and Martinelli [13], in 2011, proposed an original masking scheme that is based on SSSS that served as an alternative to Boolean masking. Goubin's scheme built upon a credible complexity-security trade-off compared to Boolean masking. Typically, the proposed SSSS masking is centered around the signal-to-noise ratio (SNR) generated by the crypto application. For example, applications involving smart card implementation tend to have a higher SNR, and it was found that the first-order of SSSS masking provided better security and less complexity than third-order Boolean masking. For hardware implementations where the noise can be reduced drastically, the same first-order of SSSS masking can produce results that are comparable to the fourth-order of Boolean masking, thereby amplifying the advantages of SSSS masking for applications of low SNR.

Following Goubin and Martinelli's [13] claim of better efficiency in their proposed scheme of SSSS masking versus Boolean masking, Coron et al. [14], in 2013, exhibited a flaw in this scheme by proving that the scheme can always be broken by a first-order side-channel analysis (SCA). In addition, Coron et al. proposed an improvement to the evaluation of the k-degree polynomial using Discrete Fourier Transformation (DFT) that reduces the evaluation time taken from $O(n^2)$ to $O(n)$, thereby effectively reducing the complexity from third order to second order.

Consider the success of reducing the computational complexity of manipulating a k^{th}-degree polynomial into a manageable polynomial of the form $f(x) = (x+\alpha)^k - b_0$, with smaller cardinality. The masking field operations in [13] similarly introduced two sensitive variables b and u following SSSS. The XOR operation with the second variable u was used to mask the sensitive variable b, where $b = (x_i, y_i), 0 \leq i \leq k(degree)$ in the following manner:

$$(x_i', y_i') \leftarrow (x_i, y_i \oplus u).$$

Multiplication by any scalar c will yield the following:

$$(x_i', y_i') \leftarrow (x_i, y_i \cdot c).$$

Working in a field of characteristic 2 squaring is $GF(256)$-linear:

$$(x_i', y_i') \leftarrow (x_i^2, y_i^2).$$

Here, it is noted that the product of two newly introduced variables that are protected by any secret sharing scheme cannot be solved using any algebraic transformation that is linear in nature, since taking the product of two k^{th}-degree polynomials will yield a polynomial with at most $2k$ degree in this finite field. In such cases, linear approximation will not be possible.

In the same research paper, Goubin and Martinelli [13] also stated that the security of SSSS against any form of SCA is based on the following selected points:

- For polynomial interpolation, at least $(k+1)$ shares are required to define a polynomial of degree k.
- The computation of $l_i(x)$ is independent of any secret share that can be found.

Through these findings by Goubin and Martinelli, the analysis in the earlier chapters can be similarly extended to the following:

- The computation of $l_i(x)$, and subsequently the secret, is independent of any public shares that can be obtained.

5.5 Monic Generator Polynomial for Secret Sharing

The analysis in Chapter 4 provides an alternate methodology to recover the secret with less-than-expected available information. It effectively reduces the evaluation of the monic polynomial to $O(n)$, since only linear algebra is involved. The objective of reducing the linearity is due to the fact that linear equations are easier to solve, which is the main motivation behind cryptanalysts' desire to approximate non-linear components with linear ones.

Although the coefficients could be generated randomly, from a security perspective, the level of security can be elevated by carefully choosing the coefficients of the generated polynomial. For improved security, the dealer should avoid generating the polynomial using successive binomial integers as its polynomial coefficients. This further amplifies the

importance of the dealer when generating the polynomial for secret sharing.

THIS PAGE INTENTIONALLY LEFT BLANK

CHAPTER 6:
Conclusion

6.1 The *Perfect* Secret Sharing Scheme

A lot of research has focused on the creation of a *perfect* secret sharing scheme. There are no known weaknesses of Shamir's Secret Sharing Scheme, other than the computational inefficiency if the generated polynomial comprises large degrees. While many improvised secret sharing schemes have proven more effective than SSSS, they have only been better under certain parameters; there is always a trade-off with some parameter of the scheme.

6.2 Future Work

Further research can be done in the following fields to enhance the efficiency of the current SSSS.

6.2.1 Ramp Secret Sharing

Ramp secret sharing involves the gradual leakage of information, subjected to a dealer-generated polynomial of degree $(t+l-1)$, where t participants have no information at the beginning. As each additional share is leaked subsequently, the bits of information that can be deciphered per share is calculated to be equal to $logq$ bits. This means that only $(t+l)$ participants can recover all secrets. This is also known as a $(t,t+l,n)$ ramp scheme, where $n \leq q-l$.

If the dealer-generated polynomial in ramp secret sharing schemes can also be reduced to the generalized form $f(x) = (x+\alpha)^k - b_0$ or the equivalent, then it may prove to be sufficient to obtain just two shares, and the secret can be recovered easily through exhaustive means of substituting the value of α.

6.2.2 Prime Numbers as Polynomial Coefficients

The dealer-generated polynomial comprises random integer coefficients. An in-depth research of prime coefficients may yield different approaches to recovering the secret because the monic polynomial now cannot be easily reduced to the generalized form

$f(x) = (x+\alpha)^k - b_0$ or the equivalent, since each of the prime coefficients $(p_1, p_2, \cdots, p_n)$ can only yield 0 when performing mod $(p_1, p_2, \cdots, p_n)$, respectively.

6.2.3 Composite Functions of Polynomials and the Fundamental Theorem of Algebra

In Section 2.3, the composite function of $f(x) = h(x) \circ g(x)$ was mooted as an alternate form to simplify the mechanics of SSSS. The function $g(x)$ was assumed to be linear, and hence, allowed the generalised form upon which this thesis analysis is based. Consider the alternate form where the dealer-generated polynomial $h(x)$ can be expressed in the form $f(x) = a_0 \times (x-\alpha)^k \times (x-\beta)^k$, by applying another linear function $g(x)$. This is also known as the Fundamental Theorem of Algebra.

APPENDIX: Diffie-Hellman Key Exchange

A.1 What Is Diffie-Hellman (D-H) Key Exchange?

In cryptography, Diffie-Hellman (D-H) key exchange is an encryption algorithm that is implemented to establish a secret between two parties. This form of key exchange is very prevalent in real-world symmetric encryption algorithms such as the Rivest-Shamir-Adleman (RSA) algorithm. It is a specific method of exchanging cryptographic keys over a public channel, but is only decipherable by the relevant parties.

The mechanics of the D-H key exchange is illustrated as such:

- Say Albert and Bernard wanted to establish a secret s, among themselves, but do not want anyone else to know about the secret.
- First, both parties have to agree on a prime number p, and a base g. Note that g is a primitive root modulo p.
- Albert then chooses a secret integer a, which only he himself knows, and computes $A = g^a \pmod{p}$.
- Bernard, like Albert, also chooses a secret integer b, which only he himself knows, and computes $B = g^b \pmod{p}$.
- Albert then sends the value of A to Bernard, and likewise, Bernard sends the value of B to Albert.
- To recompute the shared secret s, Albert computes $s = B^a \pmod{p}$, and likewise, Bernard computes $s = A^b \pmod{p}$ to obtain the secret s.

This algorithm is secure because the values of a and b are secure and known only to the relevant parties. All other values can be sent in the clear, and potentially be intercepted by other eavesdropper parties, but the eavesdropper parties will not be able to decrypt the code due to the lack of knowledge of a and b.

A.1.1 Example

- Albert and Bernard agree on $p = 23$, and $g = 5$, where 5 is a primitive root modulo 23.

- Albert chooses secret integer $a = 9$, and computes $A = g^a \pmod{p} = 5^9 \pmod{23} = 12$.
- Bernard chooses secret integer $b = 13$, and computes $B = g^b \pmod{p} = 5^{13} \pmod{23} = 2$.
- Albert sends $A = 12$ to Bernard, and receives $B = 2$ from Bernard.
- Albert then recomputes the secret $s = B^a \pmod{p} = 2^9 \pmod{23} = 6$, and Bernard computes the secret $s = A^b \pmod{p} = 12^{13} \pmod{23} = 6$.

The secret $s = 6$ can then be used as an encryption key (which is only known to the both of them) to send messages across open communications channels.

The D-H key exchange algorithm works because of the properties of modulo exponents:

$$A^b \pmod{p} = (g^a \pmod{p})^b mod p = g^{ab} \pmod{p},$$

$$B^a \pmod{p} = (g^b \pmod{p})^a mod p = g^{ba} \pmod{p},$$

$$g^{ab} \pmod{p} = g^{ba} \pmod{p}.$$

Note that for this key-exchange algorithm to work, the base g must be chosen to be a primitive root, or a generator of prime p.

List of References

[1] A. Shamir, "How to share a secret," *Commun. of the ACM*, vol. 22, no. 11, pp. 612–613, 1979.

[2] G. R. Blakley *et al.*, "Safeguarding cryptographic keys," in *Proceedings of the National Computer Conference*, vol. 48, 1979, pp. 313–317.

[3] J. B. Fraleigh, *A First Course in Abstract Algebra,* 7th ed. Pearson Education India, 2003.

[4] A. Herschfeld, "The equation $2^x - 3^y = d$," *Bulletin of the American Mathematical Society*, vol. 42, no. 4, pp. 231–234, 1936.

[5] M. Waldschmidt, "Perfect powers: Pillai's works and their developments," *Collected Works of S.S. Pillai*, vol. I, R.Balasubramaniam and R. Thangadurai, Eds. India: Ramanujan Mathematical Society, pp. xxii–xlvii, 2009.

[6] R. Stroeker and R. Tijdeman, "Diophantine equations," *Mathematisch Centrum Computational Methods in Number Theory, Pt. 2 p 321-369 (SEE N 84-17999 08-67)*, 1982.

[7] R. Taylor and A. Wiles, "Ring-theoretic properties of certain Hecke algebras," *Annals of Mathematics*, pp. 553–572, 1995.

[8] P. Mihăilescu, "Primary cyclotomic units and a proof of Catalan's conjecture," *Journal für die reine und angewandte Mathematik (Crelle's Journal)*, no. 572, 2004.

[9] H. Darmon and A. Granville, "On the equations z^m = F(x,y) and $Ax^p + By^q = Cz^r$," *Bulletin of the London Mathematical Society*, vol. 27, no. 6, pp. 513–543, 1995.

[10] M. Hall-Jr, "The diophantine equation $x^3 - y^2 = k$," *Computers in Number Theory*, vol. 38, pp. 173–198, 1971.

[11] M. A. Bennett, "On some exponential equations of S.S. Pillai," *Can. J. Mathematics*, vol. 53, no. 5, pp. 897–922, 2001.

[12] N.-F. Standard, "Announcing the Advanced Encryption Standard (AES)," *Federal Information Processing Standards Publication*, vol. 197, pp. 1–51, 2001.

[13] L. Goubin and A. Martinelli, "Protecting AES with Shamir's secret sharing scheme," in *Proc. 13th Int. Conf. Cryptographic Hardware and Embedded Syst.*, 2011, pp. 79–94.

[14] J.-S. Coron, E. Prouff, and T. Roche, *On the Use* of *Shamir's Secret Sharing against Side-Channel Analysis*. New York: Springer, 2013.

Initial Distribution List

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California